The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/29/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird, the most severe of which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 79
- Mozilla Firefox ESR versions prior to 78.1
- Mozilla Thunderbird versions prior to 78.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird, the most severe of which could allow for remote code execution. These vulnerabilities can be exploited if a user visits a specially crafted web page. Details of these vulnerabilities are as follows:

- A vulnerability exists that allows for a rogue webpage to override the injected WKUserScript. This vulnerability could result in the user downloading an unintended file. (CVE-2020-15662)
- A vulnerability exists with WKUserScript used to autofill. This vulnerability could result in leaking a password for the current domain. (CVE-2020-15661)
- A vulnerability exists with Unicode RTL order characters in downloaded file names could be used to change the extension of the file. (CVE-2020-15651)
- A vulnerability for JavaScript errors in web workers could leak the results of a cross-origin redirect. (CVE-2020-15652)
- A use-after-free vulnerability exists that could cause memory corruption and a potentially exploitable crash. (CVE-2020-6463)
- A vulnerability exists that could cause memory corruption and lead to arbitrary code execution. (CVE-2020-15659)
- A vulnerability exists to allow for a attacker-supplied DLL file to be loaded from the installation directory. (CVE-2020-15657)
- A vulnerability allowed local files to be overwritten and thus overwrite Firefox settings. (CVE-2020-15650)
- A vulnerability allowed an attacker to steal and upload local files. (CVE-2020-15649)
- JIT optimizations involving the Javascript arguments object could confuse later optimizations. (CVE-2020-15656)
- A vulnerability with Noopener links could be used to bypass security settings for websites relying on sandbox configurations that would allow popups and hosted arbitrary content. (CVE-2020-15653)
- A vulnerability exists with redirected HTTP requests that could bypass existing CORS checks. This vulnerability could lead to potential disclosure of cross-origin information. (CVE-2020-15655)
- A vulnerability exists due to improperly taking care of special characters in file downloads. (CVE-2020-15658)
- WebRTC used the memory address of a class instance as a connection identifier. (CVE-2020-6514)
- A vulnerability exists with websites that us a custom cursor using CSS which could make it look like the user is interacting with the user interface, when they are not. (CVE-2020-15654)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Mozilla to vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2020-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-32/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-34/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15649
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15650
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15651
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15652
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15653
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15654
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15655
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15656
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15657
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15658
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15659
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15661
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15662
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6463
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6514